U.S. overview of electronic signature law



The ESIGN Act, signed by President Bill Clinton on June 30, 2000, granted *electronic signatures* the same legal status as handwritten signatures throughout the United States. Electronic signatures greatly simplify the way companies gather, track and manage signatures and approvals. This paper reviews the basic requirements of

U.S. *electronic signature* law and provides some best practices that can help your company take advantage of the tremendous benefits electronic signatures offer.

What is the ESIGN Act?

The ESIGN Act of 2000 addresses electronic signatures as well as electronic records, both of which are commonly used in commerce today. Due to federal preemption, the ESIGN Act allows electronic signatures in all 50 states when federal law applies. Where federal law does not apply, every state has an electronic signature law, most following the Uniform Electronic Transactions Act (UETA).

The ESIGN Act:

- Satisfies most statutes, that require handwritten signatures on documents
- Allows the contract to be used as evidence in a court of law as long as surrounding processes are well designed and implemented and the usual elements of a contract exist
- Prevents denial of legal effect, validity or enforceability of an electronically signed document solely because it is in electronic form

What is an electronic signature?

Under the ESIGN Act, an electronic signature (or *e-signature*) is "an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." In simple terms, it is a legally recognized way to electronically indicate agreement to a contract. E-signatures streamline manual signature and approval processes by eliminating the need to print out documents, sign them in ink and scan them in order to sign. So instead of hand-delivering or mailing contracts to be signed with traditional signatures, you can send documents electronically in seconds. Approval cycles that once took weeks can now be completed in minutes. And *e-signed* agreements are much easier to track, manage, search and store than paper documents.

Requirements and best practices

Following are some requirements and best practices to consider when implementing e-signatures in your workflows.

Intent to sign

Just as with a handwritten signature, a signer must show clear intention to electronically sign an agreement. This is usually an easy requirement to satisfy. For example, signers can show intention by using a mouse to draw their signature, typing their name or clicking a button clearly labeled "I Accept" or something similar.

Consent to do business electronically

Most e-signature laws require some form of consent to do business electronically. Many enterprise e-signature solutions have some form of this consent built into the e- signature workflow. However, you may want to include additional language, so consider also including a consent clause in your agreements. For example, your agreements can contain the following clause right above the signature block:

> *The parties agree that this agreement may be electronically signed. The parties agree that the electronic signatures appearing on this agreement are the same as handwritten signatures for the purposes of validity, enforceability and admissibility.*

Record retention

The ESIGN Act enables electronic records to satisfy the record retention requirements that are imposed under other laws. The electronic records must accurately reflect the information set forth in the agreement and remain accessible in a form that allows the record to be accurately reproduced for anyone who is entitled by other laws to access the record. Often this means providing a fully executed copy to the signer or permitting the signer to download a copy of the agreement.

Opt-out clause

Signers should be given an opportunity to opt out of signing an agreement electronically. Your policy should address the procedures signers can follow if they elect to sign an agreement manually. Consider including the following clause for this purpose:

> *You may withdraw your consent to receive electronic documents, notices or disclosures at any time. In order to withdraw consent, you must notify the sending party that you wish to withdraw consent and request that your future documents, notices and disclosures be provided in paper format. To request paper copies of documents; withdraw consent to conduct business electronically and receive documents, notices or disclosures electronically; or withdraw consent to sign documents electronically, please contact the sending party by telephone, postal mail or email.*

Signed copies

All signers should receive a fully executed copy of the agreement. Many e-signature solutions automatically provide executed copies of agreements to signers as part of the approval workflow. These workflows are easily customizable, so you can choose the process that works best for your organization.

Other considerations

Here are some other things to consider.

Governing law and venue

Other countries have varying laws when it comes to e-signatures. But the good news is that e-signatures are legally valid and enforceable in nearly every industrialized country around the world. When doing business abroad, it is a good idea to designate a governing law/venue for your documents and contracts that provides the widest protection for e-signatures. Countries such as the United States, Australia, New Zealand and Canada have minimalist e-signature laws that are effective in most situations.

Advanced authentication

You can use advanced authentication options to verify signer identity before opening documents, including knowledge-based authentication, customized password or phone authentication for higher risk agreements. Knowledge-based authentication requires signers to prove their identity by answering questions unique to them. You can also authenticate signers by creating a secure, unique password they must enter before they sign. Phone authentication is effective as well. To sign, users must enter a one-time verification code that is delivered to their phone via voice or text message. This authentication data can be captured in a secure audit trail along with every other step in the signature process - including opening, signing and the IP and email address of each signer or approver – to provide clear, easily producible evidence of each party's signature.

To further enhance signer authentication, you can ask participants to sign documents with certificate-based digital IDs. Commonly referred to as *digital signatures*, this method authenticates the signer's identity through an independent Certificate Authority (CA). The signature is bound to the document, then encrypted with a tamper-evident treatment so the document itself can be used to produce evidence of each participant's signature.

Enterprise solutions

Many companies rely on enterprise e-signature solutions like *Adobe Sign* to help them customize and automate their signature and approval workflows. With it, you can set up templates that contain predefined content for different types of agreements. Also simplify authentication by selecting your desired option when you initiate agreements. And easily track, store and manage all signed documents in a central repository that is easily searchable and accessible across your organization. Adobe Sign are fully compliant with the ESIGN Act, and they make it easy to build many of the legal requirements for e-signatures right into your signature and approval process.

For more information

Thanks to laws like the ESIGN Act, e-signatures are changing the way companies do business. Signature and approval processes that once took weeks can now be completed in days or even minutes. Plus, tracking and managing signed documents is far simpler. For more information about how to effectively incorporate e-signatures into your company's workflows, consult these resources:

- *Global Overview of Electronic Signature Law*
- *Global Guide to Electronic Signature Law: Country-by-Country*
- *Developing an Effective Electronic Signature Policy*
- *ESIGN Act: A Well-Established Law Enabling Business Transformation Today*
- *Adobe Sign Solution Brief*

Adobe is pleased to provide information that can help businesses understand the legal framework of electronic signatures. However, Adobe cannot provide legal advice. Any information in this paper is not intended as legal advice and should not serve as a substitute for professional advice. You should consult an attorney regarding your specific legal questions.

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2016 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

4/16